December 30, 1996

MEMORANDUM FOR DISTRIBUTION

FROM: MARSHALL O. COMBS, DIRECTOR **/s/**
POLICY, STANDARDS AND ANALYSIS DIVISION
OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: CLARIFICATION TO THE DEPARTMENT OF ENERGY (DOE) MANUAL 5639.6A-1: CLEARING, SANITIZATION, AND DESTRUCTION OF AUTOMATED INFORMATION SYSTEMS STORAGE MEDIA, MEMORY AND HARDWARE

This clarification replaces our previous clarification to DOE Manual 5639.6A-1, dated: July 18, 1995, subject: Clarification to DOE Manual 5639.6A-1: Clearing, Sanitization, and Destruction of Automated Information Systems Storage Media, Memory and Hardware.

Attached are the Department of Energy tables, titled: Storage Media Clearing, Sanitization, and Destruction Procedures that outline the requirements for clearing, sanitization, and destruction of automated information systems storage media, memory, and hardware that have contained classified information. Also attached are two sets of instructions. One instruction titled the Partial Sanitization of Non-Removable Storage Media That Will Be Reused In A Controlled Unclassified Environment defines how to reuse large hard drives that have previously been used in a classified computing environment. The other instruction entitled Sanitization of Non-Removable Storage Media That Have Become Partially Contaminated outlines the procedures for sanitizing any non-removable storage media that has had the lesser of 20 K bytes or less than one percent of the disk capacity contaminated with classified information.

There are three significant changes in this clarification as compared to the previous clarification on this same subject. They are as follows:

1. Clearing volatile memory now requires two iterations of "power off" with a "power on" and re-initialization in between.
2. Overwriting disks for re-use in an unclassified environment now requires a record of the statistics of the overwrite and a Computer Security Site Manager (CSSM) verification before the disks can be released.
3. The acceptable volume of contamination of partially contaminated storage media where selective overwrite is acceptable for sanitization has been reduced. Previous limits were stated as 1% of the media or less. New limits are 20K bytes of data or 1% of the media, whichever is less.

If you have any questions, please contact Ray Holmer on telephone 301-903-3019.

Attachments:

1. Tables 1,2,& 3: Storage Media Clearing, Sanitization, and Destruction Procedures
2. Instruction 1: Partial Sanitization Of Non-Removable Storage Media That Will Be Reused In A Controlled Unclassified Environment
3. Instruction 2: Sanitization of Non-Removable Storage Media That Have Become Partially Contaminated

DISTRIBUTION LIST

R. E. Glass, Assistant Manager for Technical Management and Operations, AL
D. Fredrickson, Director, Personnel Security Division, AL
L. Kirkman, Acting Director, Security and Nuclear Safeguards Division, AL
D, Miller, Director, Transportation Safeguards Division, AL
D. Cook, Director, Central Training Academy, AL
T. Gradle, Director, Safeguards and Security Division, CH
M. Tolbert, Director, NBL
D.Temple, Director, Headquarters Operations Division, HQ
R. Green, Director, Special Services Division, ID
E. Adams, Director, Safeguards and Security Division, NV
H.C. White, Manager, Safeguards and Security, Yucca Mtn., NV
J. Ware, Director, Safeguards and Security Division, OR
N. Hudson, Chief, Personnel Clearance and Assurance Branch, OR
J. Medlock, Chief, Materials Control and Accountability Branch, OR
R. Mortensen, Director, Safeguards and Security Division, OAK
R. Grandfield, Compliance Team Leader, Office of Compliance Support, OHIO
E. C. Sill, Director, Contracts and Security Division, PNR*
J. Spracklen, Director, Safeguards and Security Division, RL
H. Dalton, Acting Assistant Manager for Stabilization and Disposition, RFO
W. Casey, Acting Director, Safeguards and Security Division, RFO
L. Ogletree, Director, Office of Safeguards and Security, SR
L. Brown, Director, Security Management Division, SR
R. Bartholomew, Director, Internal Security Division, SR
T. Williams, Chief, Safeguards and Classification Division, SR
G. Stefani, Jr. Director, Security and Safeguards Division, SNR*
J. Edwards, Director, Security Division, SPRO
R. L. Windus, Security Manager, BPA
T. Dembrowski, Director, Division of Safety and Security, WAPA
*THRU NR
P. Siebert, HR-433

CSOM'S DISTRIBUTION:

STEVE AUTRY, OH
CHARLES CAVAIANI, ID
LEE CHANDLER, NN-30
JACK COWDEN, NN-50, GTN
KEN CRAMER, CH
TOM MADDEN, SR
SUE FLORES, AL
TIM GLOCK, PNR THRU NE-60
DUANE GORDON, OAK
JOANNE KNOX, RF
GARY LOIACONO, RL

DONALD PROVENCHER, SNR THRU NE-60
LARRY ROUSE, NV
BILL WATSON, OAK

CSSM's DISTRIBUTION:
JOHN ADKINS
JOHN ALLEN, SAIC
JAKE APPETTA
W. L. BAXTER
GORDON BESSON, AL
M. D. BEST
GLEN BODE, CH
CONNIE BROWN, EG&G MOUND
BONNIE COCHRAN
TED COMBS, ALLIED-SIGNAL
PETE DEAN, SNL
CHRIS DEUSCHLE, FLUOR DANIEL
CHARLENE DOUGLASS, LANL
VAN DUNLOP, LLNL
ROD ELDER
CHARLES ELLISON, SR
PAUL FAVARON
RALPH FRENCH, SNL
CINDY GARNER
ROBERT GLADU
ERNEST GOVEA, FLUOR DANIEL
DAVE GRUBB, LLNL
WAYNE GUNTER
MARK HAGER, RF
BETTIE HARRIS
KATHY HAUSER, BNL
JEFF HEILMAN, PNL
JEFF HERHOLD, EG&G/EM
B. D. HYATT, LLNL
D. CRAIG JONES, SNL
KENNETH KEARLEY, WAPA
DOLORES KING
TIMOTHY LAMBKA
WILLIAM LUBIN
PEGGY MCFADDEN
NORMAL MCTYER, LLNL
BETTY MEADOWS, WSR
DARWIN MECHAM, ANL-W
JAMES MILLER, JR
CARYL MILTON, OAK
PETER MUNDING, NV

GEOF NORTHRIDGE, RF
ROSS OBLAD, LANL
D.K. PARKER, MARTIN MARIETTA
DALE PERING
MAURICE RALSTON, PNWL
DON REIGLE, ANL-E
ANTHONY SANCHEZ
JIM SCHRODER
JERRIE SHEPHERD, NN-50-GTN
DAVID SOUTHWICK, ID
JOHN STALEY, HR-441-GTN
J. C. STOLLINGS
LARRY SUPINA
CONNIE TAPIA
MARTIN THOMAS, CH-NBL
PAT THOMAS
DON THOMPSON, OAK
JIM WHYTE, WACKENHUT
FRANK ZAHROBSKY, PNR
ANTHONY ZOAR

Table 1. Storage Media Clearing, Sanitization, and Destruction Procedures

TYPE	CLEAR	Sanitize*	DESTROY
Magnetic Tape:			
Type I	1 or 2	1 or 2	5
Type II	1 or 2	2	5
Type III	1 or 2	X	5
Magnetic Disks:			
Floppies	1 or 3	1 or 2	5
Bernoullis	1 or 3	1 or 2	5
Removable Hard Disks	1 or 3	1 or 2	5 or 6
Non-removable Hard Disks **	1 or 3	1 or 2	5 or 6
Magneto-Optical			
Magneto-optic Disks: Read Only	X	X	5
Write Once, Read Many (WORM)	X	X	5
Read Many, Write Many	3	X	5
Other:			
Floptical	X	X	5
Holical-scan Tape	X	X	5
Cartridge	X	X	5
Optical	X	X	5

NOTES:

1. Degauss with a Type I degausser.
2. Degauss with a Type II degausser.
3. Overwrite all locations with any character.
4. Overwrite all locations with a character, its complement, then with any other character.
5. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanism to ensure the media is physically destroyed.
6. Remove the entire recording surfaces by sanding or applying acid.

X. No procedure authorized.

* *Sanitization of storage media or memory for release from the classified control system may not be authorized for specific categories or restrictive types of classified information. Specific guidance will be provided by the CSSM.*

** See attached instructions for Partial Sanitization of Non-Removable Storage Media That Will Be Reused In A Controlled Unclassified Environment and for Sanitization of Non-Removable Storage Media That Have Become Partially Contaminated.

Table 2. Memory Clearing, Sanitization, and Destruction Procedures

TYPE	CLEAR	SANITIZE *	DESTROY
Magnetic Bubble Memory	2	1 or 2	12
Magnetic Core Memory	2	1 or 4	12
Magnetic Plated Wire	2	3 and 5	12
Magnetic-Resistive Memory	2	X	12
Read-Only Memory (ROM)	X	X	12
Random Access Memory (Volatile)	2 or 7	6	12
Programmable ROM	X	X	12
Erasable PROM (UV PROM)	8	9 then 3 and 6	12
Electrically Alterable PROM	10	10 then 3 and 6	12
Electrically Erasable PROM (EEPROM)	11	11 then 3 and 6	12

NOTES:

1. Degauss with a Type I or Type II degausser depending on recording strength.
2. Overwrite all locations with any character.
3. Overwrite all locations with random characters.
4. Overwrite all locations with a character, its complement, then with any other or random character.
5. Sanitization not authorized if data resided in same location for more than 72 hours; sanitization not complete until overwrite has resided as long as classified data resided.
6. Check with CSSM to see if additional procedures are required.
7. A. Power "off" all sources of power for at least one minute.
   B. Power “up” and re-initialize the system including memory tests that are part of the “power up” sequence.
   C. Power "off" all sources of power again for at least one minute.
   D. Power “up” again and proceed.
   NOTE: Power “off” means the removal of all power, including battery packs.
8. Perform an ultraviolet erase according to manufacturer's recommendation.
9. Perform 8 above, but increase time requirements by factor of three.
10. Pulse all gates.
11. Perform a full chip erase (see manufacturer's data sheet for procedure).
12. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanism to ensure the memory is physically destroyed.

X. No procedure authorized.

* *Sanitization of storage media or memory may not be authorized for specific categories or restrictive types of classified information.*

Table 3. Hardware Clearing, Sanitization, and Destruction Procedures

TYPE	CLEAR	SANITIZE	DESTROY
Printer Ribbons	X	X	3
Platens	X	2	3
Toner Cartridges	1	1	3
Laser Drums	1	1	3
CRTs (Classified Burn-In)	X	X	3
Fax Machines (See notes)	4	4	3

NOTES:

1. Overwrite with three pages of randomly generated unclassified characters.
2. Chemically clean so no visible trace of data remains.
3. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanism to ensure the hardware is physically destroyed.
4. See Random Access Memory (Volatile) in Table 2 for memory procedure and CIAC advisory for hardware.

X. Not applicable.

Instruction 1: Partial Sanitization Of Non-Removable Storage Media That Will Be Reused In A Controlled Unclassified Environment

This procedure is not intended for diskettes used in work stations (Personal Computers).

When the use of a disk drive in the classified environment is no longer required, the classified drive can be overwritten and re-utilized in the unclassified environment at the site. This instruction is meant to be used in conjunction with the de-accreditation of computers. Routine use of this instruction (flip flopping) for the convenience of the site is not permitted.

Hardware Components with non-removable storage media on which classified information has been recorded may be cleared by overwriting the entire media with binary zeroes, binary ones, and then random characters from an automated random character generator.

Once cleared, the drive shall be conspicuously marked with something that indicates that the disk must be controlled as "Previously Contained Classified" and protected under a control (accountability or configuration management) system. This control system must be able to ensure that these protected magnetic platter(s) do not leave the limited security area until they are ready to be degaussed or destroyed. The Computer Security Operations Manager (CSOM) must approve the overwrite methodology. The Computer Security Site Manager (CSSM) must verify that this methodology has overwritten all classified and that the control procedures have been employed.

The overwrite program shall present information about sectors overwritten and bad sectors that cannot be overwritten.

The Computer System Security Officer (CSSO) must review the results of an overwrite to assure that sufficient overwriting has occurred and that no retrievable classified information remains before the drive is released for unclassified use.

Warning note: Normal operating systems that perform overwrite and encounter damaged disk sectors will by-pass those portions of the disk. There may be residual classified information contained in those damaged area(s). Therefore, a methodology or special software driver must be utilized that attempts to overwrite each sector despite any error messages to ensure that this classified information is overwritten or cannot be retrieved. This means that the program for each type and size of drive for each manufacturer may require a different methodology or software driver.

Instruction 2: Sanitization Of Non-Removable Storage Media That Have Become Partially Contaminated

Where a non-removable storage media has been operated in an unclassified environment, and has become contaminated with a relatively small amount of classified information, the affected area can be sanitized by overwriting the area with binary 0's, binary 1's, and then a random pattern . The CSOM must approve the overwrite methodology. The CSSM must verify that this methodology has overwritten all classified and that the control procedures have been employed

If the contamination is less than 20K bytes and less than 1 percent of the capacity of the non-removable storage media, overwriting only the contaminated areas is acceptable. If the contamination is 1 percent or greater, the non-removable storage media should be treated as if it had been operating in the classified environment, and completely sanitized in accordance with Table 1 of this clarification.

If the contamination is greater than 20K bytes and/or greater than 1 percent of the capacity of the non-removable storage media, the Computer Security Program Manager (CSPM) must approve any attempt to selectively overwrite the contaminated area and place the media back in service without a complete overwrite of the media.

The overwrite program shall provide confirmation of overwrite of the specified area and of successful completion.

NN-513	NN-512.3
Todd	Wilcher
__/__/96	__/__/96
	NN-512
	Combs
	__/__/96

KEYWORDS _____ **Distribution**
(Order Number) (Facility/Co. Name)

_____ **Clarification to the DOE Manual 5639.6A-1**
(Variance/Exception) (Subject Area)

_____ _____
(Fast Track #) (Other Keywords)

NN-512.3:holmer:ph:2528:12/23/96
C:\wpdocs\holmer\clarific.sa2
Unclassified Passport (6.1a)

Distribution:
SO: Addressee
3bcc: Stnd Ofc Cys
1bcc: NN-51 Reader

FAST TRACK ACTION

NOT A FAST TRACK ACTION

CORRESPONDENCE REVIEWER

RIGHT WRITER HAS BEEN RUN

SPELL CHECK HAS BEEN RUN

NN-512

NN-51